INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATION & MANAGEMENT

IJRCM

IJRCM

CONTENTS

CALL FOR MANUSCRIPTS

We invite unpublished novel, original, empirical and high quality research work pertaining to recent developments & practices in the areas of Computer Science & Applications; Commerce; Business; Finance; Marketing; Human Resource Management; General Management; Banking; Economics; Tourism Administration & Management; Education; Law; Library & Information Science; Defence & Strategic Studies; Electronic Science; Corporate Governance; Industrial Relations; and emerging paradigms in allied subjects like Accounting; Accounting Information Systems; Accounting Theory & Practice; Auditing; Behavioral Accounting; Behavioral Economics; Corporate Finance; Cost Accounting; Econometrics; Economic Development; Economic History; Financial Institutions & Markets; Financial Services; Fiscal Policy; Government & Non Profit Accounting; Industrial Organization; International Economics & Trade; International Finance; Macro Economics; Micro Economics; Rural Economics; Co-operation; Demography: Development Planning; Development Studies; Applied Economics; Development Economics; Business Economics; Monetary Policy; Public Policy Economics; Real Estate; Regional Economics; Political Science; Continuing Education; Labour Welfare; Philosophy; Psychology; Sociology; Tax Accounting; Advertising & Promotion Management; Management Information Systems (MIS); Business Law; Public Responsibility & Ethics; Communication; Direct Marketing; E-Commerce; Global Business; Health Care Administration; Labour Relations & Human Resource Management; Marketing Research; Marketing Theory & Applications; Non-Profit Organizations; Office Administration/Management; Operations Research/Statistics; Organizational Behavior & Theory; Organizational Development; Production/Operations; International Relations; Human Rights & Duties; Public Administration; Population Studies; Purchasing/Materials Management; Retailing; Sales/Selling; Services; Small Business Entrepreneurship; Strategic Management Policy; Technology/Innovation; Tourism & Hospitality; Transportation Distribution; Algorithms; Artificial Intelligence; Compilers & Translation; Computer Aided Design (CAD); Computer Aided Manufacturing; Computer Graphics; Computer Organization & Architecture; Database Structures & Systems; Discrete Structures; Internet; Management Information Systems; Modeling & Simulation; Neural Systems/Neural Networks; Numerical Analysis/Scientific Computing; Object Oriented Programming; Operating Systems; Programming Languages; Robotics; Symbolic & Formal Logic; Web Design and emerging paradigms in allied subjects.

Anybody can submit the **soft copy** of unpublished novel; original; empirical and high quality **research work/manuscript** *anytime* in *M.S. Word format* after preparing the same as per our **GUIDELINES FOR SUBMISSION**; at our email address i.e. infoijrcm@gmail.com or online by clicking the link **online submission** as given on our website (*FOR ONLINE SUBMISSION, CLICK HERE*).

GUIDELINES FOR SUBMISSION OF MANUSCRIPT

1.   **COVERING LETTER FOR SUBMISSION**:

                                                                                              DATED: _____

   THE EDITOR

   IJRCM

   Subject: **SUBMISSION OF MANUSCRIPT IN THE AREA OF   .**

   (e.g. Finance/Mkt./HRM/General Mgt./Engineering/Economics/Computer/IT/ Education/Psychology/Law/Math/other, please specify)

   DEAR SIR/MADAM

   Please find my submission of manuscript entitled '_____' for possible publication in one of your journals.

   I hereby affirm that the contents of this manuscript are original. Furthermore, it has neither been published elsewhere in any language fully or partly, nor is it under review for publication elsewhere.

   I affirm that all the co-authors of this manuscript have seen the submitted version of the manuscript and have agreed to their inclusion of names as co-authors.

   Also, if my/our manuscript is accepted, I agree to comply with the formalities as given on the website of the journal. The Journal has discretion to publish our contribution in any of its journals.

NAME OF CORRESPONDING AUTHOR	:
Designation	:
Institution/College/University with full address & Pin Code	:
Residential address with Pin Code	:
Mobile Number (s) with country ISD code	:
Is WhatsApp or Viber active on your above noted Mobile Number (Yes/No)	:
Landline Number (s) with country ISD code	:
E-mail Address	:
Alternate E-mail Address	:
Nationality	:

NOTES:

a) The whole manuscript has to be in *ONE MS WORD FILE* only, which will start from the covering letter, inside the manuscript. *pdf. version* **is liable to be rejected without any consideration**.

b) The sender is required to mention the following in the **SUBJECT COLUMN of the mail**:

New Manuscript for Review in the area of (e.g. Finance/Marketing/HRM/General Mgt./Engineering/Economics/Computer/IT/ Education/Psychology/Law/Math/other, please specify)

c) There is no need to give any text in the body of mail, except the cases where the author wishes to give any **specific message** w.r.t. to the manuscript.

d) The total size of the file containing the manuscript is expected to be below **1000 KB**.

e) **Abstract alone will not be considered for review** and the author is required to submit the **complete manuscript** in the first instance.

f) *The journal gives acknowledgement w.r.t. the receipt of every email within twenty four hours* and in case of non-receipt of acknowledgment from the journal, w.r.t. the submission of manuscript, within two days of submission, the corresponding author is required to demand for the same by sending a separate mail to the journal.

g) The author (s) name or details should not appear anywhere on the body of the manuscript, except the covering letter and the cover page of the manuscript, in the manner as mentioned in the guidelines.

2. **MANUSCRIPT TITLE**: The title of the paper should be **bold typed**, **centered** and **fully capitalised**.

3. **AUTHOR NAME (S) & AFFILIATIONS**: Author (s) **name**, **designation**, **affiliation** (s), **address**, **mobile/landline number** (s), and **email/alternate email address** should be given underneath the title.

4. **ACKNOWLEDGMENTS**: Acknowledgements can be given to reviewers, guides, funding institutions, etc., if any.

5. **ABSTRACT**: Abstract should be in **fully italicized text**, ranging between **150** to **300 words**. The abstract must be informative and explain the background, aims, methods, results & conclusion in a **SINGLE PARA**. *Abbreviations must be mentioned in full*.

6. **KEYWORDS**: Abstract must be followed by a list of keywords, subject to the maximum of **five**. These should be arranged in alphabetic order separated by commas and full stop at the end. All words of the keywords, including the first one should be in small letters, except special words e.g. name of the Countries, abbreviations.

7. **JEL CODE**: Provide the appropriate Journal of Economic Literature Classification System code (s). JEL codes are available at www.aeaweb.org/econlit/jelCodes.php, however, mentioning JEL Code is not mandatory.

8. **MANUSCRIPT**: Manuscript must be in *BRITISH ENGLISH* prepared on a standard A4 size *PORTRAIT SETTING PAPER*. *It should be free from any errors i.e. grammatical, spelling or punctuation. It must be thoroughly edited at your end*.

9. **HEADINGS**: All the headings must be bold-faced, aligned left and fully capitalised. Leave a blank line before each heading.

10. **SUB-HEADINGS**: All the sub-headings must be bold-faced, aligned left and fully capitalised.

11. **MAIN TEXT**:

THE MAIN TEXT SHOULD FOLLOW THE FOLLOWING SEQUENCE:

INTRODUCTION

REVIEW OF LITERATURE

NEED/IMPORTANCE OF THE STUDY

STATEMENT OF THE PROBLEM

OBJECTIVES

HYPOTHESIS (ES)

RESEARCH METHODOLOGY

RESULTS & DISCUSSION

FINDINGS

RECOMMENDATIONS/SUGGESTIONS

CONCLUSIONS

LIMITATIONS

SCOPE FOR FURTHER RESEARCH

REFERENCES

APPENDIX/ANNEXURE

The manuscript should preferably range from *2000 to 5000 WORDS*.

12. **FIGURES & TABLES:** These should be simple, crystal **CLEAR**, **centered**, **separately numbered** & self explained, and **titles must be above the table/figure**. **Sources of data should be mentioned below the table/figure**. *It should be ensured that the tables/figures are referred to from the main text.*

13. **EQUATIONS/FORMULAE:** These should be consecutively numbered in parenthesis, horizontally centered with equation/formulae number placed at the right. The equation editor provided with standard versions of Microsoft Word should be utilised. If any other equation editor is utilised, author must confirm that these equations may be viewed and edited in versions of Microsoft Office that does not have the editor.

14. **ACRONYMS:** These should not be used in the abstract. The use of acronyms is elsewhere is acceptable. Acronyms should be defined on its first use in each section: Reserve Bank of India (RBI). Acronyms should be redefined on first use in subsequent sections.

15. **REFERENCES:** The list of all references should be alphabetically arranged. *The author (s) should mention only the actually utilised references in the preparation of manuscript* and they are supposed to follow Harvard Style of Referencing. **Also check to make sure that everything that you are including in the reference section is duly cited in the paper**. The author (s) are supposed to follow the references as per the following:

- All works cited in the text (including sources for tables and figures) should be listed alphabetically.

- Use (**ed.**) for one editor, and (**ed.s**) for multiple editors.

- When listing two or more works by one author, use --- (20xx), such as after Kohl (1997), use --- (2001), etc, in chronologically ascending order.

- Indicate (opening and closing) page numbers for articles in journals and for chapters in books.

- The title of books and journals should be in italics. Double quotation marks are used for titles of journal articles, book chapters, dissertations, reports, working papers, unpublished material, etc.

- For titles in a language other than English, provide an English translation in parenthesis.

- *Headers, footers, endnotes* and *footnotes* should **not be used** in the document. However, **you can mention short notes to elucidate some specific point**, which may be placed in number orders after the references.

PLEASE USE THE FOLLOWING FOR STYLE AND PUNCTUATION IN REFERENCES:

BOOKS

- Bowersox, Donald J., Closs, David J., (1996), "Logistical Management." Tata McGraw, Hill, New Delhi.

- Hunker, H.L. and A.J. Wright (1963), "Factors of Industrial Location in Ohio" Ohio State University, Nigeria.

CONTRIBUTIONS TO BOOKS

- Sharma T., Kwatra, G. (2008) Effectiveness of Social Advertising: A Study of Selected Campaigns, Corporate Social Responsibility, Edited by David Crowther & Nicholas Capaldi, Ashgate Research Companion to Corporate Social Responsibility, Chapter 15, pp 287-303.

JOURNAL AND OTHER ARTICLES

- Schemenner, R.W., Huber, J.C. and Cook, R.L. (1987), "Geographic Differences and the Location of New Manufacturing Facilities," Journal of Urban Economics, Vol. 21, No. 1, pp. 83-104.

CONFERENCE PAPERS

- Garg, Sambhav (2011): "Business Ethics" Paper presented at the Annual International Conference for the All India Management Association, New Delhi, India, 19–23

UNPUBLISHED DISSERTATIONS

- Kumar S. (2011): "Customer Value: A Comparative Study of Rural and Urban Customers," Thesis, Kurukshetra University, Kurukshetra.

ONLINE RESOURCES

- Always indicate the date that the source was accessed, as online resources are frequently updated or removed.

WEBSITES

- Garg, Bhavet (2011): Towards a New Gas Policy, Political Weekly, Viewed on January 01, 2012 http://epw.in/user/viewabstract.jsp

SECURE DATA TRANSMISSION IN MOBILE AD-HOC NETWORK USING RDSDV PROTOCOL

A. P. PANDE
ASST. PROFESSOR
DEPARTMENT OF INFORMATION TECHNOLOGY
P.V.P.I.T
SANGLI

A. U. PATIL
ASST. PROFESSOR
PAD. VASANTRAODADA PATIL INSTITUTE OF TECHNOLOGY
BUDHGAON

ABSTRACT

In mobile ad hoc network (MANET) is an autonomous system of mobile nodes. The nodes are free to move arbitrarily. Due to lack of a centralized secure infrastructure, the communication is prone to security attacks and the nodes can be easily compromised. Security has become one of the major issues for data communication over wired and wireless networks so various security-enhanced measures have been proposed to improve the security of data transmission over public networks.The objective of this work is toimprove routing security we represent a proactive mechanism as Randomized routing that explores the existence of multiple routes and forces packets to take alternate paths randomly from its neighbors that is a Randomize delivery path for secure data transmission. We maintain neighboring nodes of each node by sending hello packets. Then we find out delivery path from neighboring nodes by random operation excluding previous hop which is maintained as history node. Protocol RDSDV is implemented to randomize delivery paths and compared the proactive routing protocols DSDV and RDSDV for different number of nodes. The performance of these protocols is measured under a particular scenario on the basis of three metrics as Packet delivery ratio, e2e delay and jitter. This work is implemented in Network Simulator version 2.35.

KEYWORDS
mobile nodes, packets, routing, security.

1. INTRODUCTION
ireless cellular systems have been in use since 1980s. Wireless systems operate with the aid of a centralized supporting structure such as an access point. These access points assist the wireless users to keep connected with the wireless system, when they roam from one place to the other. The presence of a fixed supporting structure limits the adaptability of wireless systems. In other words, the technology cannot work effectively in places where there is no fixed infrastructure. Future generation wireless systems will require easy and quick deployment of wireless networks. This quick network deployment is not possible with the existing structure of current wireless systems.

Wireless networking is an emerging technology that allows users to access information and services electronically, regardless of their geographic position. Wireless networks can be classified in two types: Centralized approach Or Infrastructure Networks and Decentralized approach or Infrastructure less (ad-hoc) Networks[1]. Infrastructure network consists of a network with fixed and wired gateways. A mobile host communicates with a bridge in the network (called base station) within its communication radius. The mobile unit can move geographically while it is communicating. When it goes out of range of one base station, it connects with new base station and starts communicating through it. This is called handoff. In this approach the base stations are fixed.

In contrast to infrastructure based wireless network, in ad-hoc networks all nodes are mobile and can be connected dynamically in an arbitrary manner. A MANET is a collection of wireless mobile nodes forming a temporary network without using any existing infrastructure or any administrative support. The wireless ad-hoc networks are self-creating, self-organizing and self-administrating. The nodes in an ad-hoc networkcan be a laptop, cell phone, PDA or any other device capable of communicating with those nodes located within its transmission range. The nodes can function as routers, which discover and maintain routes to other nodes. The ad-hoc network may be used in emergency search-and-rescue operations, battlefield operations and data acquisition in inhospitable terrain.

Nodes in mobile ad-hoc network are free to move and organize themselves in an arbitrary fashion. Each user is free to roam about while communication with others. The path between each pair of the users may have multiple links and the radio between them can be heterogeneous. This allows an association of various links to be a part of the same network.In ad-hoc networks, dynamic routing protocol must be needed to keep the record of high degree of node mobility, which often changes the network topology dynamically and unpredictably.

The security of communication in ad hoc wireless networks is important, especially in military applications. The absence of any central coordination mechanism and shared wireless medium makes MANETs more vulnerable to digital/cyber-attacks than wired networks. These attacks are generally classified into two types: passive and active attacks. Passive attacks do not influence the functionality of a connection. An adversary aims to interfere in a network and read the transmitted information without changing it. If it is also possible for the adversary to interpret the captured data, the requirement of confidentiality isviolated. It's difficult to recognize passive attacks because under such attacks the network operates normally.

In general, encryption.[2] is used to combat such attacks. Active attacks aim to change or destroy the data of a transmission or attempt to influence the normal functioning of the network. Active attacks when performed from foreign networks are referred to as external attacks. If nodes from within the adhoc network are involved, the attacks are referred to as internal attacks

2. LITERATURE REVIEW
C. Villamizar [3] proposed the delivery of secret information across insecure networks. They proposed an end-to-end data delivery scheme called secure protocol for Reliable data delivery (SPREAD).The basic idea of SPREAD is to improve the confidentiality by using multipath routing.

D. Clark et al [4] proposed a simple algorithm called Adaptive Multi-Path routing (AMP) algorithm for dynamic traffic engineering within autonomous systems. In contrast to related multipath routing proposals, AMP does not employ a global perspective of the network in each node. Here available information is restricted to a local scope, through which signaling overhead and memory consumption in routers are reduced.

S. Kent, et al. [5] explored a security enhanced dynamic routing algorithm which randomizes the paths in which the data packets are sent. This algorithm is efficient and compatible with mostly used routing protocols like Routing Information Protocol (RIP) and Destination-sequenced Distance Vector (DSDV) protocol for wired and wireless networks respectively. Both the above stated protocols need to exchange extra control messages. But control messages are avoided in security enhanced dynamic routing. The main objective in it is to minimize the path similarity i.e. the path taken by the consecutive packets must not be the same.Virtual Private Networks [5], or VPNs, have been used as a way to securely interconnect a (typically small) number of sites. While private networks use dedicated lines, VPNs try to implement private networks atop a publicly-accessible communication infrastructure like the Internet. VPNs typically employ some combination of encryption, authentication, and access control techniques to allow participating sites to communicate securely.

The emergence of IPsec [6] as a IETF standardized protocol has prompted VPN solutions to use IPsec as the underlying network-layer protocol. Secure BGP (S-BGP) [7] makes use of public key and authorization infrastructure, as well as IPsec to verify the authenticity and authorization of control traffic generated by the Border Gateway Protocol (BGP).

Onion routing [7] is another approach to security that focuses on hiding the identities of communicators. It uses several layers of encryption, where each layer is used to encrypt the transmission between routers on each end of a link. Because of the many layers of encryption, routers are unable to decrypt the data or even the source and destination addresses. All that a router can decipher is the next-hop information. While onion routing is very effective for anonymity, it is not very efficient: each connection must be built and torn down, routers must encode and decode packets, and memory-intensive source routing is used. More recently, motivated by constant distributed denial-ofservice attacks (DDoS) to the Internet, several research efforts have focused on addressing routing-level security.

Center track [8] uses an IP overlay network composed of Center track routers to log packets. Using the resulting logs, it is possible to reconstruct the path traversed by attacker's packets.

IP trace back [9] tries to accomplish the same goal of tracking DDoS attacks by tracing packets back to their source. The IP trackback mechanism uses probabilistic. Packet marking at routers which allows a victim to identify the path(s) attack traffic traversed without support from service providers/administrators.

Another related effort is the Resilient Overlay Networks (RON) project [11] whose goal is to improve the performance and robustness of network-layer routing. RON nodes monitor current routing paths and decide whether to choose other routes (by selecting alternate application-layer paths through other RON nodes) to meet application-specific performance requirements.

Existing work on security-enhanced data transmission includes the designs of cryptography algorithms and system infrastructures and security-enhanced routing methods. Their common objectives are often to defeat various threats over the Internet, including eavesdropping, spoofing, session hijacking, etc.Among many well-known designs for cryptography based systems, the IP Security (IPSec) and the Secure Socket Layer are popularly supported and implemented in many systems and platforms. Although IPSec and SSL do greatly improve the security level for data transmission, but they introduce substantial overheads which is unavoidable. Especially on gateway/host performance and effective network bandwidth. For example, the data transmission overhead is 5 cycles/byte over an Intel Pentium II with the Linux IP stack alone, and the overhead increases to 58cycles/byte when Advanced Encryption Standard (AES) is adopted for encryption/decryption. Differentfrom the past work on the designs of cryptography algorithms and system infrastructures, weimplementedRandomize delivery paths algorithm for data transmission

3. RDSDV IMPLEMENTATION

The objective of implemented work is to a Randomize delivery path for secure data transmission. The delivery of a packet with the destination at a node in order to minimize the probability that packets are eavesdropped over a specific link, a randomization process for packet deliveries. In this process, the previous next-hop for the source node s is identified in the first step of the process. Then, the process randomly picks up a neighboring node as the next hop for the current packet transmission. The exclusion for the next hop selection avoids transmitting two consecutive packets in the same link, and the randomized pickup prevents attackers from easily predicting routing paths for the coming transmitted packets.The existing system relies on distance information exchanged among neighboring nodes for the seeking of routing paths. in distance-vector-based implementations, those based on rip, each node n_i maintains a routing table in which each entry is associated with a unique destination node (t), an estimated minimal cost to send a packet to t , and the next node cost to send a packet to t (next hop). we modify routing table entry by adding set of node candidates for the next hop and as a set of entries records the history for packet deliveries through the node n_i to the destination node t.

4. RANDOMIZED NEXT HOP SELECTION ALGORITHM

1: Let hs be the used nexthop for the previous packet delivery for the source node s.
2: prepare neighbor list of node s by sending hello packets.
3: if neighbor list is > 1 then
4: Randomly choose a node x from neighbor list
If x equal to hs then repeat from step 3 three times
else
send the packet pkt to the node x.
5: set hs as node x, and update the routing table of node n.
7: Send the packet pkt to hs.
9: else
10: Randomly choose a node y from neighbor list and send the packet pkt to the node y.
11: set hs as y, and update the routing table of Ni.
12: end if

5. EXPRIMENTAL RESULT

SIMULATION PARAMETERS

Following table shows network simulation parameters which are configured in tcl script as network interface, queue type and simulation area and others.

TABLE 1: NETWORK SIMULATION PARAMETER

Parameters	Values
Network interface/channel type	Wireless
Radio-propagation model	TwoRayGround
Network interface type	Phy/WirelessPhy
packet size	512bytes
Interface queue type	Queue/DropTail/PriQueue
Max packet in IFQ	50
Number of mobile Nodes	50
Simulation area size	1000*1000
Simulation duration	150 second
Transmission range of each node	250 m
Mobility model	Random
Routing protocols	RDSDV ,DSDV

The performance of the two protocols under different scenario are Compared on the different performance metrics as PDR, average end to end delay and Jitter.

TABLE 2: NETWORK PERFORMANCE METRICS

Sr.no	Performance Metric	Description
1	PDR (packet Delivery Ratio)	PDR =∑ Number of packet receive / ∑ Number of packet send
2	Average E2E Delay (End to End delay)	End to End Delay = ∑ (arrive time – send time) / ∑ Number of nodes
3	Jitter	AVERAGE JITTER= ∑ [((recvtime(j)-sendtime(j))-(recvtime(i)-sendtime(i)))/(j-i)]/ number of nodes

We find out experimental results on above performance metric in following scenario as for Random position and random node movement. We consider different topology size with 30 to 110 nodes. Results of performance metric are compared in using Microsoft Excel tool.

SCENARIO 1

Under this scenario, we consider network size as 1000 X 1000 m

1.   Jitter variation for network size 1000 x 1000

TABLE 3: JITTER VARIATION FOR NETWORK SIZE 1000 X 1000

Number of Nodes	Jitter of DSDV Protocol	Jitter of Randomized DSDV
30	0.001883	0.002108
50	0.002121	0.004522
70	0.002130	0.003985
90	0.001875	0.005734
110	0.002143	0.003625

FIGURE 1: JITTER VALUES VARIATION FOR NETWORK SIZE 1000 X 1000 M

Table 3 shows the jitter variation for network size 1000X1000 m for nodes 30 to 110. Figure 1 shows the graph based on table 3.These results shows the jitter values of RDSDV protocol are more than the values of DSDV. Hence the path variation more than existing DSDV protocol.

1)   PACKET DELIVERY RATIO VARIATION

TABLE 4: PDR VARIATION FOR NETWORK SIZE 1000 X 1000

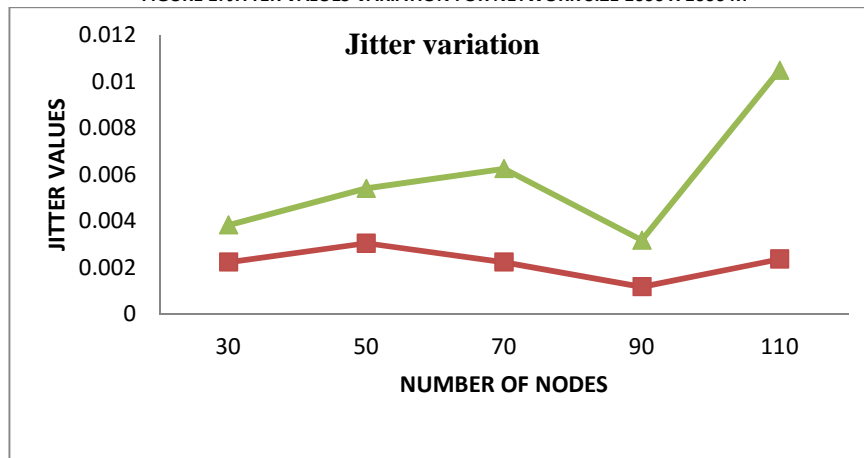| Number of Nodes	PDR of DSDV Protocol	PDR of Randomized DSDV
30	99.79	99.84
50	99.38	99.65
70	99.32	99.70
90	99.51	99.91
110	99.35	99.85

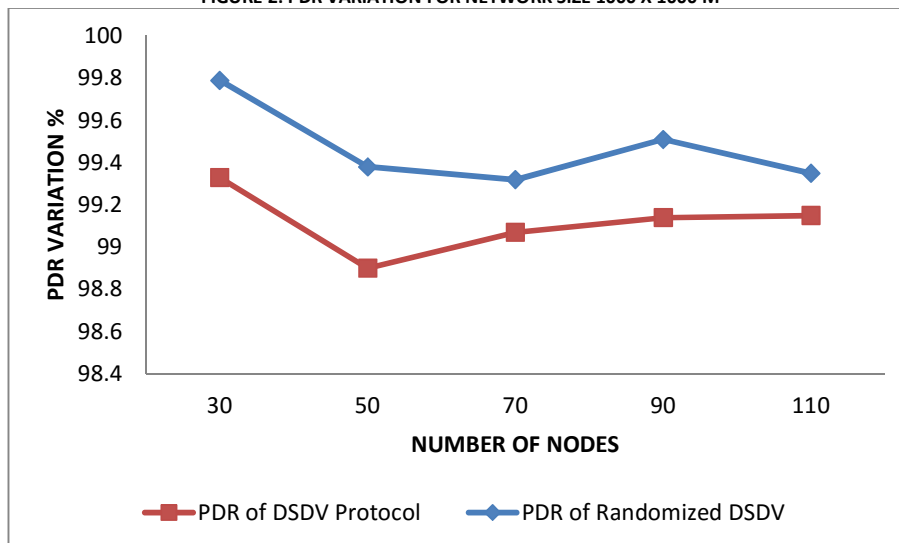**FIGURE 2: PDR VARIATION FOR NETWORK SIZE 1000 X 1000 M**

Table 4 shows the PDR variation for network size 1000 X 1000 m for nodes 30 to 110. Figure 2 shows the graph based on table 4.These results shows the PDR values of RDSDV protocol are more than the values of DSDV. Hence the PDR variation more than existing DSDV protocol.

2. **AVERAGE END TO END DELAY VARIATION**

TABLE 5: AVERAGE END TO END DELAY VARIATION FOR NETWORK SIZE 1000 X 1000

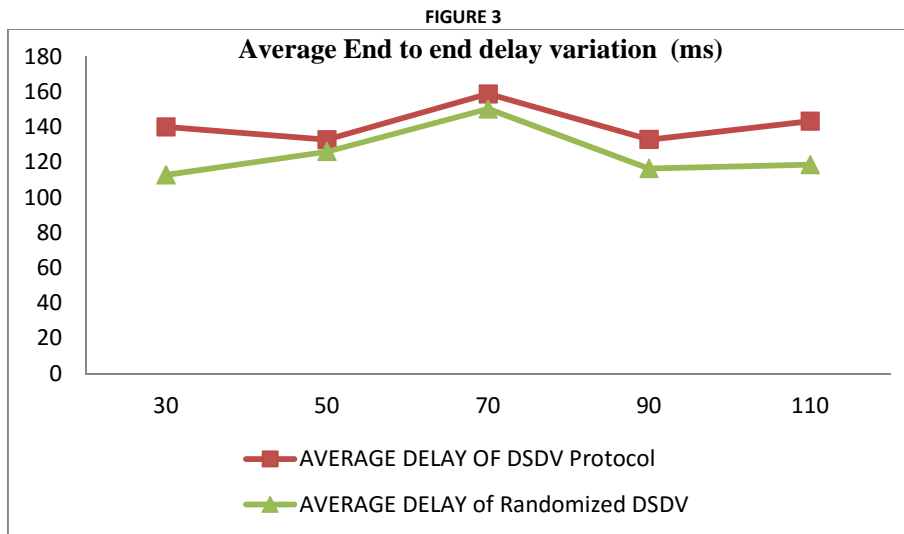| Number of Nodes	AVERAGE DELAYOF DSDV Protocol	AVERAGE DELAY of Randomized DSDV
30	140.14	112.81
50	123.88	126.11
70	152.92	150.33
90	132.98	116.54
110	143.35	118.68

FIGURE 3

Table 5 Shows the Average end to end delay variation for network size 1000 X 1000 m for nodes 30 to 110. Figure 3 shows the graph based on table 5. These results shows the average end to end delay values of RDSDV protocol are less than the values of DSDV. Hence the average end to end delay variation of RDSDV protocol is less than existing DSDV protocol.

6. CONCLUSION

To protect information and resources from attacks and misbehavior. We implemented randomized delivery path protocol. In order to minimize the probability that packets are eavesdropped over a specific link, a randomize process for packet deliveries, randomly picks up a neighboring node as the next hop for the current packet transmission. The exclusion for the next hop selection avoids transmitting two consecutive packets on the same link and the randomized pickup prevents attackers from easily predicting routing paths for the coming transmitted packets.

Experimental results are drawn on different scenarios with different numbers of nodes and network size and nodes mobility speed shows that jitter value is greater and increases as number of nodes increases hence prove that each packet transmitted at different path to destination. As jitter values are more means more path variations for packet delivery to destination which combat security attacks. The PDR and End to End Delay metrics of RDSDV protocol is closer to the metrics for DSDV protocol under same topology. Hence we conclude that security attacks can be avoided by this process without reducing performance.

REFERENCES

1. Y. Zhang, V. Paxson, and S. Shenker, "The stationary of internet path properties: Routing, loss, and throughput," tech. rep., ACIRI, May, 2000.
2. D. Thaler and C. Hopps, "Multipath issues in unicast and multicast nexthop selection," RFC 2991, Nov. 2000.
3. C. Villamizar, "Ospf optimized multipath (ospf-omp)," draft-ietf-ospfomp- 03, p. 46, June 1999.
4. J. Saltzer, D. Reed, and D. Clark, "End-to-end arguments in system design," AMC Trans. on Computer Systems, vol. 2, no. 4, pp. 195–206, 1984.
5. S. Kent, C. Lynn, J. Mikkelson, and K. Seo, "Secure border gateway protocol (s-BGP) - real world performance and deployment issues," in Proceedings of NDSS 2000, 2000.
6. M. K. Reiter andA. D. Rubin, "Crowds: AnonymityforWeb transactions," ACM Trans. on Information and System Security, vol. 1, pp. 66–92, 1998.
7. P. F. Syverson, M. G. Reed, and D. M. Goldschlag, "Onion routing access configurations," in DISCEX 2000: Proceedings of the DARPA Information Survivability Conference and Exposition, vol. I, pp. 34–40, Jan. 2000.
8. R. Stone, "CenterTrack: An IP overlay network for tracking DoS floods," in 9th USENIX Security Symposium, 2000.
9. S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Practical network support for IP traceback," in Proceedings of the 2000 ACM SIGCOMM Conference, (Stockholm, Sweden), pp. 295–306, August, 2000.
10. D. G. Andersen, H. Balakrishnan, M. F. Kaashoek, and R. Morris, "Resilient overlay networks," in Proc. 18th ACM SOSP, (Banff, Canada),2001.
11. J. P. Hespanha and S. Bohacek, "Preliminary results in routing games," in Proc. Of the 2001 American Control Conference, June, 2001.
12. S. D. Patek and D. P. Bertsekas, "Stochastic shortest path games," SIAM J Contr. Optimization, vol. 37, pp. 803–824, 1999.
13. The VINT Project, a collaboration between UC Berkeley, LBL, USC/ISI and Xerox PARC, "The ns manual (formerly ns Notes and Documentation)." http://www.isi.edu/nsnam/ns/ns-documentation.html, Oct. 2000.

REQUEST FOR FEEDBACK

Dear Readers

At the very outset, International Journal of Research in Computer Application & Management (IJRCM) acknowledges & appreciates your efforts in showing interest in our present issue under your kind perusal.

I would like to request you to supply your critical comments and suggestions about the material published in this issue as well as on the journal as a whole, on our E-mail **infoijrcm@gmail.com** for further improvements in the interest of research.

If you have any queries, please feel free to contact us on our E-mail **infoijrcm@gmail.com**.

I am sure that your feedback and deliberations would make future issues better – a result of our joint effort.

Looking forward an appropriate consideration.

With sincere regards

Thanking you profoundly

Academically yours

Sd/-
Co-ordinator

DISCLAIMER

The information and opinions presented in the Journal reflect the views of the authors and not of the Journal or its Editorial Board or the Publishers/Editors. Publication does not constitute endorsement by the journal. Neither the Journal nor its publishers/Editors/Editorial Board nor anyone else involved in creating, producing or delivering the journal or the materials contained therein, assumes any liability or responsibility for the accuracy, completeness, or usefulness of any information provided in the journal, nor shall they be liable for any direct, indirect, incidental, special, consequential or punitive damages arising out of the use of information/material contained in the journal. The journal, neither its publishers/Editors/ Editorial Board, nor any other party involved in the preparation of material contained in the journal represents or warrants that the information contained herein is in every respect accurate or complete, and they are not responsible for any errors or omissions or for the results obtained from the use of such material. Readers are encouraged to confirm the information contained herein with other sources. The responsibility of the contents and the opinions expressed in this journal are exclusively of the author (s) concerned.

ABOUT THE JOURNAL

In this age of Commerce, Economics, Computer, I.T. & Management and cut throat competition, a group of intellectuals felt the need to have some platform, where young and budding managers and academicians could express their views and discuss the problems among their peers. This journal was conceived with this noble intention in view. This journal has been introduced to give an opportunity for expressing refined and innovative ideas in this field. It is our humble endeavour to provide a springboard to the upcoming specialists and give a chance to know about the latest in the sphere of research and knowledge. We have taken a small step and we hope that with the active co-operation of like-minded scholars, we shall be able to serve the society with our humble efforts.

Our Other Journals